UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/540,613	03/31/2000	Carl M. Ellison	042390.P8628	2175

8791 7590 02/12/2004

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD, SEVENTH FLOOR
LOS ANGELES, CA 90025

EXAMINER	
TRAN, ELLEN C	

ART UNIT	PAPER NUMBER
2134	13

DATE MAILED: 02/12/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/540,613	ELLISON ET AL.	
	Examiner	Art Unit	
	Ellen C Tran	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 March 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-60* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-60* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5, 7-10* .
4) ☐ Interview Summary (PTO-413) Paper No(s) _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

Detailed Action

1. This action is responsive to communication: original application filed 31 March 2000.

2. Claims 1-60 are currently pending in this application. Claims 1, 16, 31, and 46 are independent claims.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language

4. **Claims 1, 16, 31, and 46** are rejected under 35 U.S.C. 102(e) as being anticipated by Barnett U.S. Patent No. 6,292,874 (hereinafter '874).

As to independent claim 16, "A method comprising: initializing a chipset in a secure environment for an isolated execution mode by an initialization storage, the secure environment having a plurality of executive entities and being associated with an isolated memory area accessible by at least one processor, the at least one processor having a plurality of threads and operating in one of a normal execution mode and the isolated execution mode, the executive entities including a processor executive (PE) handler; and 8 storing PE handler data corresponding to

the PE handler in a PE handler storage, the PE handler data including a PE handler image to be loaded into the isolated memory area after the chipset is initialized, the loaded PE handler image corresponding to the PE handler" is taught in '874 col. 2 line 47-65 "Generally, a memory management unit is disclosed for a single-chip data processing circuit, such as a smart card. The memory management unit (i) partitions a homogeneous memory device to achieve heterogeneous memory characteristics for various regions of the memory device, and (ii) restricts access of installed applications executing in the microprocessor core to predetermined memory ranges. Thus, the memory management unit imposes firewalls between applications and permits hardware checked partitioning of the memory. The memory management unit provides two operating modes for the processing circuit. In a secure kernel mode, the programmer can access all resources of the device including hardware control. In an application mode, the memory management unit translates the virtual memory address used by the software creator into the physical address allocated to the application by the operating system in a secure kernel mode during installation".

As to independent claims 1, this claim is the apparatus comprising the same method of claim 16 and is similarly rejected along the same rationale.

As to independent claim 31, this claim is a computer program product comprising the same method as claim 16 and is similarly rejected along the same rationale.

As to independent claim 46, this claim is a system comprising the same method as claim 16 and is similarly rejected along the same rationale.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. **Claims 2, 3, 17, 18, 32, 33, 47, and 48** are rejected under 35 U.S.C. 103(a) as being unpatentable over '874 in view of Panwar et al. U.S. Patent No. 6,035,374 (hereinafter '374).

As to dependent claim 17, "storing a chipset mode indicating a mode of operation of the chipset in a mode storage; and writing the chipset mode into the mode storage" is taught in '874 col. 2, lines 58-65 "The memory management unit provides two operating modes for the processing circuit. In a secure kernel mode, the programmer can access all resources of the device including hardware control. In an application mode, the memory management unit translates the virtual memory address used by the software creator into the physical address allocated to the application by the operating system in a secure kernel mode during installation"; the following in not taught in '874:

- **"further comprises: storing a thread count in a thread count storage indicating number of threads currently operating in the isolated**

execution mode; updating the thread count when the initialization storage is accessed" however '374 teaches "ISU 206 (shown in greater detail in FIG. 8) is operative to schedule and dispatch instructions as soon as their dependencies have been satisfied into an appropriate execution unit (e.g., integer execution unit (IEU) 208, or floating point and graphics unit (FGU) 210). ISU 206 also maintains trap status of live instructions. ISU 206 may perform other functions such as maintaining the correct architectural state of processor 102, including state maintenance when out-of-order instruction processing is used. ISU 206 may include mechanisms to redirect execution appropriately when traps or interrupts occur and to ensure efficient execution of multiple threads where multiple threaded operation is used. Multiple thread operation means that processor 102 is running multiple substantially independent processes simultaneously ... state machines 301 are implemented in ISU 206 by maintaining virtual processor status information in ISU 206. Although other functional units use the thread ID to implement multiprocessors in accordance with the present invention, ISU 206 uses the virtual processor status information ... Hence, to ease circuit complexity and improve operation speed, it is advantageous to implement state machines 301 in ISU 206" in col. 13, lines 9-35";

- **It would have been obvious** to one of ordinary skill in the art at the time of the invention to modify the method of initializing a chipset with multiprocessors with isolated and normal execution modes taught in '874 to include a method for counting processors being utilized. One of ordinary skill in

the art would have been motivated to perform such a modification because the method of executing coded instruction in a dynamically configurable multiprocessor is well known in the art see '374 (col. 4, lines 38 et seq.) "A processor in accordance with the present invention includes a processor creation unit responsive to a processor create command to output signals indicating a current processor configuration and plurality of virtual or logical processors each virtual processor ...The state machines maintain processor status information representative of whether the processor is available to receive and execute instructions. The processor further includes status logic analyzing expected latency of instructions on each processor and updating the state machine corresponding to any processor having an instruction with an expected latency greater than a preselected threshold".

As to dependent claim 18, "further comprising: storing identifiers of the executive entities operating in the isolated execution mode, the identifiers being read only when in lock; storing a lock pattern indicating the identifiers in lock; and locking the identifiers based on the lock pattern" is taught in '874 col. 2, lines 47-58 "The memory management unit provides two operating modes for the processing circuit. In a secure kernel mode, the programmer can access all resources of the device including hardware control. In an application mode, the memory management unit translates the virtual memory address used by the software creator into the physical address allocated to the application by the operating system in a secure kernel mode during installation".

As to dependent claims 2, 3, 32, 33, 47, and 48 these claims incorporated substantially similar subject matter as cited in claims 17-18 above and are similarly rejected along the same rationale.

7. **Claims 4-14, 19-29, 34-44, and 49-59** are rejected under 35 U.S.C. 103(a) as being unpatentable over '874 in view of '374, in further view of Pub. No. U.S. 20002/0007456 (hereinafter '456) by Peinado et al.

As to dependent claim 19, "; the following in not taught the combination of teachings of '874 and '374: **"further comprising: storing a fused key used in handling the executive entities in a fused key storage; and storing isolated settings used to configure the isolated execution mode"** however '456 teaches "In the present invention, a secure processor for a computing device is operable in a normal mode and a preferred mode, and includes a security kernel for being instantiated on the processor when the processor enters into the preferred mode and a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode. The security kernel employs the accessed security key during the preferred mode to authenticate a secure application on the computing device, and allows the processor to be trusted to keep hidden a secret of the application" on page 2 paragraph 18.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of initializing a chipset with multiprocessors with isolated and normal execution modes and counting the status of the processors taught in the combination of '874 and '374 to include a

key mapped to the isolated location. One of ordinary skill in the art would have been motivated to perform such a modification because security keys with enforcement architecture are often used when managing digital rights see '456 (page 1 paragraphs 10-11) "When a user attempts to render the digital content on a computing device, the rendering application invokes a Digital Rights Management (DRM) system on such user's computing device. If the user is attempting to render the digital content for the first time, the DRM system either directs the user to a license server to obtain a license to render such digital content in the manner sought, or transparently obtains such license from such license server without any action necessary on the part of the user. The license includes: a decryption key (KD) that decrypts the encrypted digital content".

As to dependent claim 20, "wherein the executive entities further include a processor executive (PE) and an operating system executive (OSE)" is taught in '374 col. 4, lines 38-48 "A processor in accordance with the present invention includes a processor creation unit responsive to a processor create command to output signals indicating a current processor configuration and plurality of virtual or logical processors each virtual processor having a first set of execution resources that are uniquely identified with the virtual processor and a second set of execution resources that are shared amongst the plurality of virtual processors".

As to dependent claim 21, "wherein the chipset mode is one of an initialization waiting mode to indicate the chipset is waiting for initialization, a PE initialization in-progress mode to indicate the PE is

being executed, a PE initialization completion mode to indicate the PE is completed, an OSE loaded mode to indicate the OSE has been loaded, a closing mode to indicate the isolated execution mode is closed, and a failure mode to indicate a failure" is disclosed in '374 col. 4, lines 48-50 "A plurality of state machines responsive to the processor creation unit are provided, each corresponding to a selected one of the plurality of virtual processors. The state machines maintain processor status information representative of whether the processor is available to receive and execute instructions".

As to dependent claim 22, "wherein initializing the chipset comprises returning an updated thread count when the chipset mode does not represent the failure mode, the updated thread count being one of an incremented thread count and a decremented thread count; and returning a current thread count when the chipset mode represents the failure mode" is disclosed in '374 col. 10, lines 18-36 "Once a branch is resolved, the address of the path this branch actually follows is communicated from IEU 208 and compared against the predicted path address store in the BT ADDRESS fields. If these two addresses differ, those instructions down the mispredicted path are flushed from the processor and IFU 202 redirects instruction fetch down the correct path identified in the BNT ADDRESS field using the BRT input to MUX 505. Once a branch is resolved, the BHT value is updated using the BHT index and BHT value stored in BRT 515. In the example of FIG. 5, each entry in BHT 519 is a two-bit saturating counter. When a predicted branch is resolved taken, the entry used to predict this outcome is incremented. When a

predicted branch is resolved not taken, the entry in BHT 519 is decremented. Other branch prediction algorithms and techniques may be used in accordance with the present invention, so long as care is taken to duplicate resources on a processor-by-processor basis where those resources are used exclusively by a given processor".

As to dependent claim 23, "wherein initializing the chipset further Comprises: returning the incremented thread count when one of the threads enrolls in the isolated execution mode; and returning the decremented thread count when one of the enrolled threads withdraws from the isolated execution mode" is taught in '374 col. 13, lines 9-15 "ISU 206 (shown in greater detail in FIG. 8) is operative to schedule and dispatch instructions as soon as their dependencies have been satisfied into an appropriate execution unit (e.g., integer execution unit (IEU) 208, or floating point and graphics unit (FGU) 210). ISU 206 also maintains trap status of live instructions".

As to dependent claim 24, "wherein writing the chipset mode comprises writing the chipset mode corresponding, to a failure mode when the thread count reaches a thread limit" is shown in '374 col. 4, lines 51-55 "The processor further includes status logic analyzing expected latency of instructions on each processor and updating the state machine corresponding to any processor having an instruction with an expected latency greater than a preselected threshold".

As to dependent claim 25, "wherein the PE handler data further include a PE handler identifier, a PE handler size, and a PE handler address" is disclosed in '374 col. 11, lines 3-19 "IFU 202 includes instruction marker circuitry 507 for analyzing the fetched instructions to determine selected information about the instructions. Marker unit 507 is also coupled to processor create unit 200. This selected information, including the thread identification (i.e., the virtual processor identification) generated by processor create unit 200, is referred to herein as "instruction metadata". In accordance with the present invention, each fetch bundle is tagged with a thread identification for use by downstream functional units. Other metadata comprises information about, for example, instruction complexity and downstream resources that are required to execute the instruction. The term "execution resources" refers to architectural register space, rename register space, table space, decoding stage resources, and the like that must be committed within processor 102 to execute the instruction".

As to dependent claim 26, "wherein the PE handler storage is a non-volatile memory" is taught in '374 col. 10, lines 18-23 "Once a branch is resolved, the address of the path this branch actually follows is communicated from IEU 208 and compared against the predicted path address store in the BT ADDRESS fields. If these two addresses differ, those instructions down the mispredicted path are flushed from the processor".

As to dependent claim 27, "wherein the fused key is returned when the fused key storage is read in the initialization waiting mode" is shown in

'456 page 15, paragraph 220 "the root entity returns the license server public key (PU-LS) to such license server 24 encrypted with the private root key"

As to dependent claim 28, " wherein the fused key is programmed at manufacturing time to a random value" is disclosed in '456 page 21 paragraph 290 "In the present invention, the secure processor 64 is constructed to include a security (CPU) key 66 physically hard-wired (permanently stored) thereinto, and the security kernel 68 is also physically hard-wired thereinto, where only the security kernel 68 can access the CPU key 66. Such physical hard-wiring may be performed during manufacturing of the secure processor 64 and may be done in any appropriate manner without departing from the spirit and scope of the present invention. Such physical hardwiring is known or should be apparent to the relevant public and therefore need not be described herein in any detail. For example, the secure processor 64 may be manufactured with storage space 70 for a CPU key 66 and a security kernel 68, where the storage space 70 is in the form of ROM to be pre-programmed by the manufacturer".

As to dependent claim 29, "further comprising: storing a status value of an isolated unlock pin used in restoring a root key from the fused key" is taught in '456 page2, paragraphs 17 and 18 "Once the downloaded license has been stored in the DRM system license store, the user can render the digital content according to the rights conferred by the license and specified in the license terms. When a request is made to render the digital content, the black box is caused to decrypt the decryption key and license terms, and a DRM

system license evaluator evaluates such license terms. The black box decrypts the encrypted digital content only if the license evaluation results in a decision that the requester is allowed to play such content. The decrypted content is provided to the rendering application for rendering. In the present invention, a secure processor for a computing device is operable in a normal mode and a preferred mode, and includes a security kernel for being instantiated on the processor when the processor enters into the preferred mode and a security key accessible by the instantiated security kernel when the processor is operating in the preferred mode. The security kernel employs the accessed security key during the preferred mode to authenticate a secure application on the computing device, and allows the processor to be trusted to keep hidden a secret of the application"

As to dependent claims 4-14, 34-44, and 49-59 these claims incorporated substantially similar subject matter as cited in claims 19-29 above and are similarly rejected along the same rationale.

8. **Claims 15, 30, 45, and 60** are rejected under 35 U.S.C. 103(a) as being unpatentable over '874 in view, in view of '374, in view of '456, in further view of Ellison et al. U.S. Patent No. 6,507,904 (hereinafter '904).

As to dependent claim 30, the following is not taught in the combination of teachings from '874, '374 and '456: **"wherein the isolated settings include an isolated base value, in isolated mask value, and a processor executive entry address, the isolated base and mask values defining the isolated memory area"** however '904 teaches "The system of claim 29 wherein the at

least one parameter is one of an isolated feature word, an execution mode word, a logical processor value, an isolated setting including a mask value and a base value, a frame, an exit physical address, an entry physical address, and a processor nub loader physical address" in claim 30 col. 16, lines 62-67.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of initializing a chipset with multiprocessors with isolated and normal execution modes, counting the status of the processors and utilizing a key taught in the combination of '874, '374, and '456 to include masked values. One of ordinary skill in the art would have been motivated to perform such a modification because mask values are used with isolated processors see '904 (col. 3, lines 59 et seq.) "One principle for providing security in a computer system or platform is the concept of an isolated execution architecture. The isolated execution architecture includes logical and physical definitions of hardware and software components that interact directly or indirectly with an operating system of the computer system or platform. An operating system and the processor may have several levels of hierarchy, referred to as rings, corresponding to various operational modes".

As to dependent 15, 45, and 60 these claims incorporated substantially similar subject matter as cited in claim 30 above and are similarly rejected along the same rationale.

Conclusion

9. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Browne U.S. Patent No. 6,272,533 issued dated: Aug. 7, 2001

Ellison et al. U.S. Patent No. 6,633,963 issued dated: Oct. 14, 2003

10. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ellen C Tran whose telephone number is (703) 305-8917. The examiner can normally be reached on 6:30 am to 3:30 pm. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory A Morse can be reached on (703) 308-4789. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 306-5484.

NORMAN M. WRIGHT
PRIMARY EXAMINER

Ellen. Tran
Patent Examiner
Technology Center 2134
January 30, 2004